Affine Equivalence of Quartic Monomial Rotation Symmetric Boolean Functions in Prime Power Dimension

Pantelimon Stănică

Naval Postgraduate School,
Department of Applied Mathematics,
Monterey, CA 93943–5216, USA;
pstanica@nps.edu

Abstract

In this paper we analyze and exactly compute the number of affine equivalence classes under permutations for quartic monomial rotation symmetric functions in prime and prime power dimensions.

Keywords: Boolean functions, circulant matrices, affine equivalence, permutations, prime powers.
Mathematics Subject Classification [2010]: 94A60, 94C10, 06E30

1. Introduction

An n-variable Boolean function f is a map from the n dimensional vector space $\mathbb{F}_2^n = \{0,1\}^n$ into the two-element field $\mathbb{F}_2$, that is, an n-variable Boolean function f is a multivariate polynomial over $\mathbb{F}_2$. Denoting the addition operator over $\mathbb{F}_2$ by '+', a Boolean function can be thought as a multivariate polynomial, called the *algebraic normal form* (ANF)

$$f(x_1,\ldots,x_n) = a_0 + \sum_{1\le i\le n} a_i x_i + \sum_{1\le i<j\le n} a_{ij} x_i x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$. The maximum number of variables in a monomial is called the (*algebraic*) *degree*, and it is denoted by $deg(f)$. If all monomials in its ANF have the same degree, the Boolean function is said to be *homogeneous*.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. Define

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 JAN 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A ffine Equivalence of Quartic Monomial Rotation Symmetric Boolean Functions in Prime Power Dimension	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Applied Mathematics Department,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In this paper we analyze and exactly compute the number of a ne equiva- lence classes under permutations for quartic monomial rotation symmetric functions in prime and prime power dimensions.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**22**	

the scalar product of $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ both in $\mathbb{F}_2^n$, by $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$. The *(Hamming) weight*, denoted by $wt(\mathbf{x})$, of a binary string $\mathbf{x}$ is the number of ones in $\mathbf{x}$, and the *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is the number of positions where $\mathbf{x}, \mathbf{y}$ differ. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$). The nonlinearity of an n-variable function f is the minimum distance to the entire set of affine functions, which is known to be bounded from above by $2^{n-1} - 2^{n/2-1}$.

We define the (right) rotation operator ρ_n on a vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ by $\rho_n(x_1, x_2, \ldots, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$. Hence, ρ_n^k acts as a k-cyclic rotation on an n-bit vector. A Boolean function f is called *rotation symmetric* if for each input $(x_1, \ldots, x_n)$ in $\mathbb{F}_2^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$, for $1 \leq k \leq n$. That is, the rotation symmetric Boolean functions (RSBF) are invariant under cyclic rotation of inputs. A partition of some cardinality g_n is generated by $G_n(x_1, \ldots, x_n) = \{\rho_n^k(x_1, \ldots, x_n) | 1 \leq k \leq n\}$, and so, the number of n-variable RSBFs is 2^{g_n}. It was shown [11] that $g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$, where ϕ is Euler's totient function. We refer to [8, 9, 11] for the formula on how to calculate the number of partitions with weight w, say $g_{n,w}$, for arbitrary n and w.

A rotation symmetric function $f(x_1, \ldots, x_n)$ can be written as

$$a_0 + a_1 x_1 + \sum a_{1j} x_1 x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$, and the existence of a representative term $x_1 x_{i_2} \ldots x_{i_l}$ implies the existence of all the terms from $G_n(x_1 x_{i_2} \ldots x_{i_l})$ in the ANF. This representation of f (not unique, since one can choose any representative in $G_n(x_1 x_{i_2} \ldots x_{i_l})$) is called the *short algebraic normal form* (SANF) of f. If the SANF of f contains only one term, we call such a function a *monomial rotation symmetric* (MRS) function. Certainly, the number of terms in the ANF of a monomial rotation symmetric function is a divisor of n (see [11]).

We say that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ in $\mathcal{B}_n$ are *affine equivalent* if $g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b})$, where $A \in GL_n(\mathbb{F}_2)$ ($n \times n$ nonsingular matrices over the finite field $\mathbb{F}_2$ with the usual operations) and $\mathbf{b}$ is an n-vector over $\mathbb{F}_2$. We say $f(\mathbf{x}A + \mathbf{b})$ is a *nonsingular affine transformation* of $f(\mathbf{x})$. It is easy to see that if f and g are affine equivalent, then they have the same weight and nonlinearity: $wt(f) = wt(g)$ and $N_f = N_g$ (these are examples of *affine invariants*).

There are cases, when it is known that these invariants are also sufficient (two quadratic functions are affine equivalent if and only if their weights

and nonlinearity are the same–see [3], for example). However, in general, for higher degrees, that it is not the case.

2. Background on *S*-equivalence

In [2] the authors introduced the notion of *S-equivalence* $f \overset{S}{\sim} g$, which is the affine equivalence of monomial rotation symmetric (MRS) functions f, g under permutation of variables (we will write here $f \sim g$, for easy displaying).

An $n \times n$ matrix C is *circulant*, denoted by $\mathrm{C}(c_1, c_2, \ldots, c_n)$, if all its rows are successive circular rotations of the first row, that is,

$$C = \begin{pmatrix} c_1 & c_2 & \ldots & c_n \\ c_n & c_1 & \ldots & c_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ c_2 & c_3 & \ldots & c_1 \end{pmatrix}.$$

On the set $\mathcal{C}_n$ of circulant matrices an equivalence relation was introduced in [2]: for $A_1 = \mathrm{C}(a_1, \ldots, a_n)$, $A_2 = \mathrm{C}(b_1, \ldots, b_n)$, then $A_1 \approx A_2$ if and only if $(a_1, \ldots, a_n) = \rho_n^k(b_1, \ldots, b_n)$, for some $0 \leq k \leq n-1$. It was shown that the set of equivalence classes (the equivalence class of $\mathrm{C}(a_1, a_2, \ldots, a_n)$ is denoted by $\mathrm{C}\langle a_1, a_2, \ldots, a_n\rangle$, or $\langle \mathrm{C}(a_1, a_2, \ldots, a_n)\rangle$) form a commutative monoid (under the natural operation $\langle A\rangle \cdot \langle B\rangle := \langle AB\rangle$). Moreover, the previous operation partitions the invertible $n \times n$ circulant matrices into equivalence classes, say $\mathcal{C}_n^*/_{\approx}$, and consequently, $(\mathcal{C}_n^*/_{\approx}, \cdot)$ becomes a group.

Let $f = x_1 x_{j_2} \cdots x_{j_d} + x_2 x_{j_2+1} \cdots x_{j_d+1} + \cdots + x_n x_{j_2-1} \cdots x_{j_d-1}$ be an MRS function of degree d, with the SANF $x_1 x_{j_2} \cdots x_{j_d}$. We associate to f the following (unique) circulant matrix equivalence class

$$A_f = \langle \mathrm{C}(\overset{1}{\underset{\downarrow}{1}}, 0, \ldots, \overset{j_2}{\underset{\downarrow}{1}}, 0, \ldots, 0, \overset{j_3}{\underset{\downarrow}{1}}, \ldots, 0, \overset{j_d}{\underset{\downarrow}{1}}, \ldots, 0)\rangle, \tag{1}$$

where the 1 bits (indicated above) appear in positions given by the indices in the SANF monomial of f.

For a binary (row) vector $(a_1, a_2, \ldots, a_n)$ of dimension n, we let $\Delta(a_1, a_2, \ldots, a_n) \equiv \{i \,|\, a_i = 1\}$, and by abuse of notation, $\Delta(C(\mathbf{a})) = \Delta(\mathbf{a})$. Similarly, for a single monomial term $x_{i_1} x_{i_2} \cdots x_{i_d}$ of degree d in n variables, we define $\Delta(x_{i_1} x_{i_2} \cdots x_{i_d}) \equiv \{i_j \,|\, j = 1, 2, \ldots, d\}$. We can also extend this to the MRS function with this SANF, $f = x_{i_1} x_{i_2} \cdots x_{i_d}$, as $\Delta(f) = \Delta(x_{i_1} x_{i_2} \cdots x_{i_d})$, which is not unique, but we prefer (so not to complicate the notation) to consider all such sets equal under a cyclic

rotation permutation of the indices. That is, for A_f as in (1), then $\Delta(f) = \{1, j_2, \ldots, j_d\} = \{2, j_2 + 1, \ldots, j_d + 1\} = \cdots$. Therefore, for a fixed n, any such particular set Δ of indices generates a unique monomial $x_{i_1} x_{i_2} \cdots x_{i_d}$ in n binary variables, a unique n-dimensional bit vector $\mathbf{a}$, the corresponding unique matrix equivalence class $C\langle \mathbf{a} \rangle$, and the corresponding unique MRS function $f = x_{i_1} x_{i_2} \cdots x_{i_d}$ (SANF) such that $A_f = C\langle \mathbf{a} \rangle$.

We now consider another type of equivalence between circulant matrices, that can be extended to the equivalence classes we have defined. For two circulant matrices A, B, if there are permutation matrices P, Q such that $PA = BQ$, then A and B are called P-Q equivalent. It is known in that case that AA^T and BB^T are similar matrices (in fact, there exists a permutation matrix which conjugates one to the other) [12]. Moreover, it is rather straightforward to see that $AA^T = \sum_{i,j \in \Delta(A)} G^{i-j}$, where $A = \mathrm{C}(a_1, \ldots, a_n)$.

The notion of P-Q equivalence extends naturally from circulant matrices to equivalence classes, as any product of permutation matrices is also a permutation matrix, and any two representative matrices A_1, A_2 of an equivalence class $\langle A \rangle$ are related by a rotation of the row order.

The following two results are essential in our investigation.

Theorem 2.1 (Canright–Chung–Stănică [2])**.** *Two MRS Boolean functions f, g in n variables are S-equivalent if and only if their corresponding circulant matrix equivalence classes A_f and A_g are P-Q equivalent.*

Theorem 2.2 (Wiedemann–Zieve [12])**.** *Let A, B be two $n \times n$ 0/1-circulants of weight at most 5 with first rows support indices $\Delta(A)$, respectively, $\Delta(B)$, where n is odd. Then the following are equivalent:*

1. *There exist $u, v \in \mathbb{Z}_n$ such that $\gcd(u, n) = 1$ and $\Delta(A) = u\Delta(B) + v$.*
2. *A, B are P–Q equivalent.*
3. *There is an $n \times n$ permutation matrix P such that $AA^T = PBB^TP^{-1}$.*
4. *The matrices AA^T, BB^T are similar.*

It is known [12] that if the weight of A, B is $2, 3$, then Theorem 2.2 holds without constraints. If the weight is $k \in \{4, 5\}$, then Theorem 2.2 holds for dimensions n whose prime factors are greater than $2k(k-1)$ (that is, if $k = 4$, the prime factors should be greater than 24).

For easy reference, based upon the previous theorems, we often write interchangeably $f \sim g$ (for two MRS f, g), or $\Delta(A_f) \sim \Delta(A_g)$ (if there exist $u, v \in \mathbb{Z}_n$ such that $\gcd(u, n) = 1$ and $\Delta(A) = u\Delta(B) + v$).

In this paper we will find the number of equivalence classes (and representatives of these classes) for quartic (degree 4) MRS (that is, their SANF

is $f = x_1x_ix_jx_k$ with $\Delta(f) = \{1, i, j, k\}$) in prime and prime power dimensions. We mention that the result for prime dimension appears in a recent paper of Cusick and Cheon [6]. We give here a rather short proof of that result.

3. Counting quartic equivalence classes for prime dimension

For easy displaying, we sometimes write $\frac{a}{b}$ to mean ab^{-1} in some obvious environment; we also adopt the convention throughout that working in some $\mathbb{Z}_{p^\ell}$, $p^t x^{-1}$ exists if $p^\alpha \| x = p^\alpha y$, $0 \le \alpha \le t$, and $p^t x^{-1} := p^{t-\alpha} y^{-1}$.

We start with a descriptive lemma describing some representatives of the equivalence classes. Throughout this paper we use the "capital mod" notation a Mod n to mean the unique integer $b \in \{1, 2, \ldots, n\}$ such that $b \equiv a \bmod n$. We use the notation $p^s \| m$ to mean the highest power of p that divides m.

Lemma 3.1. *The S-equivalence class of any quartic MRS h with $\Delta(h) = \{1, i, j, k\}$ where either $\gcd(i-1, n) = \gcd(j-1, n) = \gcd(k-1, n) = \gcd(i-j, n) = \gcd(k-j, n) = \gcd(k-i, n) = 1$, contains a quartic MRS g with $\Delta(g) = \{1, 2, m, r\}$. If $n = p^\ell$, $\ell \ge 2$, where p is an odd prime and $\gcd(i-1, n) \ne 1$, $\gcd(j-1, n) \ne 1$, $\gcd(k-1, n) \ne 1$, then the class of h will not contain any MRS function g with $\Delta(g) = \{1, 2, m, r\}$, rather it will contain one with $\Delta(g) = \{1, p^s+1, m, r\}$, where $p^s \| \gcd(i-1, j-1, k-1)$, $1 \le s \le \ell - 1$, $p^s | (m-1)$ and $p^s | (r-1)$. Moreover, every such class with a representative of support $\{1, p^s+1, Ap^s+1, Bp^s+1\}$ will contain one with support $\{1, p^s+1, ap^s+1, bp^s+1\}$ with $\gcd(ab, p) = 1$ where p divides either both of $(a-1), (b-1)$ or none, or $p | \gcd(a, b-1)$ or $p | \gcd(b, a-1)$. Furthermore, two MRS with supports $\{1, p^s+1, ap^s+1, bp^s+1\}$, $\gcd(ab, p) = 1$, respectively, $\{1, p^s+1, a'p^{s+1}+1, (b'p+1)p^s+1\}$ cannot be S-equivalent.*

Proof. We first assume that at least one of $\gcd(i-1, n) = 1$, $\gcd(j-1, n) = 1$, $\gcd(k-1, n) = 1$, $\gcd(i-j, n) = 1$, $\gcd(k-j, n) = 1$, $\gcd(k-i, n) = 1$ holds. By Theorem 2.1 and Theorem 2.2 it will be sufficient to show that for every such MRS h with $\Delta(h) = \{1, i, j, k\}$, there exists u, v such that $u\Delta(h) + v = \{1, 2, m, r\}$, for some m, r. Solving the corresponding 24 systems we obtain the possibilities for (m, r, u, v):

$$\left\{\frac{i+j-2}{i-1}, \frac{i+k-2}{i-1}, \frac{1}{i-1}, \frac{i-2}{i-1}\right\}; \qquad \left\{\frac{i+k-2}{i-1}, \frac{i+j-2}{i-1}, \frac{1}{i-1}, 1+\frac{1}{1-i}\right\};$$
$$\left\{\frac{i+j-2}{j-1}, \frac{j+k-2}{j-1}, \frac{1}{j-1}, \frac{j-2}{j-1}\right\}; \qquad \left\{\frac{i+k-2}{k-1}, \frac{j+k-2}{k-1}, \frac{1}{k-1}, 1+\frac{1}{1-k}\right\};$$
$$\left\{\frac{j+k-2}{j-1}, \frac{i+j-2}{j-1}, \frac{1}{j-1}, \frac{j-2}{j-1}\right\}; \qquad \left\{\frac{j+k-2}{k-1}, \frac{i+k-2}{k-1}, \frac{1}{k-1}, 1+\frac{1}{1-k}\right\};$$

$$\left\{\frac{-2i+j+1}{1-i}, \frac{-2i+k+1}{1-i}, \frac{1}{1-i}, 2+\frac{1}{i-1}\right\}; \quad \left\{\frac{-2i+k+1}{1-i}, \frac{-2i+j+1}{1-i}, \frac{1}{1-i}, 2+\frac{1}{i-1}\right\};$$
$$\left\{\frac{1-i}{j-1}+2, \frac{-2j+k+1}{1-j}, \frac{1}{1-j}, 2+\frac{1}{j-1}\right\}; \qquad \left\{\frac{1-i}{k-1}+2, \frac{1-j}{k-1}+2, \frac{1}{1-k}, 2+\frac{1}{k-1}\right\};$$
$$\left\{\frac{-2j+k+1}{1-j}, \frac{1-i}{j-1}+2, \frac{1}{1-j}, 2+\frac{1}{j-1}\right\}; \qquad \left\{\frac{1-j}{k-1}+2, \frac{1-i}{k-1}+2, \frac{1}{1-k}, 2+\frac{1}{k-1}\right\};$$
$$\left\{\frac{i-1}{i-j}+1, -\frac{-2i+j+k}{i-j}, \frac{1}{j-i}, \frac{i}{i-j}+1\right\}; \qquad \left\{\frac{2i-k-1}{i-k}, \frac{2i-j-k}{i-k}, \frac{1}{k-i}, \frac{2i-k}{i-k}\right\};$$
$$\left\{\frac{i-1}{j-i}+2, \frac{i-2j+k}{i-j}, \frac{1}{i-j}, \frac{i}{j-i}+2\right\}; \qquad \left\{\frac{i-1}{k-i}+2, \frac{i+j-2k}{i-k}, \frac{1}{i-k}, \frac{i}{k-i}+2\right\};$$
$$\left\{\frac{j-1}{j-k}+1, \frac{j-i}{j-k}+1, \frac{1}{k-j}, \frac{j}{j-k}+1\right\}; \qquad \left\{\frac{j-1}{k-j}+2, \frac{i+j-2k}{j-k}, \frac{1}{j-k}, \frac{j}{k-j}+2\right\};$$
$$\left\{\frac{-2i+j+k}{j-i}, \frac{i-1}{i-j}+1, \frac{1}{j-i}, \frac{i}{i-j}+1\right\}; \qquad \left\{\frac{i-j}{i-k}+1, \frac{i-1}{i-k}+1, \frac{1}{k-i}, \frac{i}{i-k}+1\right\};$$
$$\left\{\frac{i-2j+k}{i-j}, \frac{i-1}{j-i}+2, \frac{1}{i-j}, \frac{i}{j-i}+2\right\}; \qquad \left\{\frac{i+j-2k}{i-k}, \frac{i-1}{k-i}+2, \frac{1}{i-k}, \frac{i}{k-i}+2\right\};$$
$$\left\{\frac{j-i}{j-k}+1, \frac{j-1}{j-k}+1, \frac{1}{k-j}, \frac{j}{j-k}+1\right\}; \qquad \left\{\frac{i+j-2k}{j-k}, \frac{j-1}{k-j}+2, \frac{1}{j-k}, \frac{j}{k-j}+2\right\}.$$

We easily see that if $\gcd(i-1,n)=1$, taking $u=(i-1)^{-1}, v=u-1$, then $\{1,i,j,k\} \sim \{1,2,m,r\}$ via u,v; similarly, for $\gcd(j-1,n)=1$, or $\gcd(k-1,n)=1$, etc.

Next assume that for $s \geq 1$, $p^s \| \gcd(i-1, j-1, k-1)$ (and consequently, it also divides $j-i, k-i, k-j$). Without loss of generality, we assume that $p^s \| (i-1)$, and so $i-1=p^s t$ for some $t \not\equiv 0 \pmod{p}$ (the other cases are similar). By taking $u=t^{-1}, v=1-u, m=1+(j-1)u, r=1+(k-1)u$ (all are Mod p^ℓ), then we see that $\{1,i,j,k\} \sim \{1, p^s+1, m, r\}$. Certainly $p^s | m-1=(j-1)t^{-1}, p^s | r-1=(k-1)t^{-1}$, since $p^s \| \gcd(i-1, j-1, k-1)$. Moreover, for every class, which we have now shown that has a representative of the form $\{1, p^s+1, ap^s+1, bp^s+1\}$, if $p|a$, we can find a representative $\{1, p^s+1, a'p^s+1, b'p^s+1\}$ with $p \not| a'$ (that is seen by taking the affine transformation based on $u=-1, v=2+p^s$ and so, $a'=1-a$, $b'=1-b$, $\gcd(a',p)=1$).

The next claim follows easily by finding appropriate values of u,v,a,b such that $u\{1, p^s+1, Ap^s+1, Bp^s+1\}+v = \{1, p^s+1, ap^s+1, bp^s+1\}$ with $\gcd(ab,p)=1$ and $p|\gcd(a-1,b-1)$, or $p|(a-1)$ and $p|b$, or $p|(b-1)$ and $p|a$:
(i) If $p \not| A(A-1)B(B-1)$, respectively, we can take $u=(B-1)^{-1}$, $v=1-(p^s+1)(AB-1)^{-1}$, $a=-(B-1)^{-1}$, $b=(A-1)(B-1)^{-1}$, so $p \not| ab(a-1)(b-1)$ and $p \not| (a-b)$ (Case B_3 and B_5 later).
(ii) If $p|(A-1), p|(B-1)$, then $p|(A-B)$, $p \not| AB$; If $p|A, p|B$, then we can take $u=-1, v=2+p^s$, $a=1-A$, $b=1-B$; thus, $p|(a-1), p|(b-1)$, and $p|(a-b)$, $p \not| ab$ (both of these instances are equivalent and constitute Case

B_1 later).
(*iii*) If $p|(B-1)$ and $p \not| A(A-1)$ (similarly for $p|(A-1)$ and $p \not| B(B-1)$), then take $u = A^{-1}, v = 1 - A^{-1}$, $a = A^{-1}, b = BA^{-1}$; thus, $p|(a-b)$, $p \not| ab(a-1)(b-1)$ (Case B_2 and B_4 later).
(*iv*) If $p|A$, $p \not| B$, $p \not| (B-1)$ (similarly, for $p|B$, $p \not| A$, $p \not| (A-1)$), the same transformation as in (*i*) gives us a representative with $p \not| ab(a-1)(b-1)$ and $p|(a-b)$.
(*v*) If $p|A, p|(B-1)$ (similarly for $p|B, p|(A-1)$), then we have a representative of the form $\{1, p^s+1, ap^{s+1}+1, (bp+1)p^s+1\}$ ($a = A/p, b = (B-1)/p$) (Case C later).

Thus, a representative of such a class can be taken of the form $\{1, p^s + 1, ap^s+1, bp^s+1\}$ with $\gcd(ab, p) = 1$, $p|\gcd(b-1, a-1)$, or $p \not| (a-1)(b-1))$.

Now, given two classes with supports $\{1, p^s + 1, ap^s + 1, bp^s + 1\}$ with $\gcd(ab, p) = 1$, $p|(a-1)$ or $(b-1)$, respectively, $\{1, p^s + 1, a'p^{s+1} + 1, (b'p + 1)p^s + 1\}$, and listing the possibilities of (a', b', u) with $\gcd(u, p) = 1$ that could potentially map the first support unto the second via the corresponding affine transformation with some shift v, we see that in every instance, either a, or b must be divisible by p, and that is impossible. Thus, the two classes are not S-equivalent. □

We denote by $E(p)_k$ the number of distinct equivalence classes of quartic MRS in p variables, for $p \equiv k \pmod{12}$, where $k = 1, 5, 7, 11$. Although this result is shown in [6], we give a much shorter alternate proof here.

Theorem 3.2. *Let $p \geq 11$ be a prime. Then the number of S-equivalence classes of quartic MRS in p variables is*

$$E(p)_1 = \frac{p^2 - 2p + 25}{24}, E(p)_5 = \frac{p^2 - 2p + 9}{24},$$
$$E(p)_7 = \frac{p^2 - 2p + 13}{24}, E(p)_{11} = \frac{p^2 - 2p - 3}{24}.$$

Proof. Since p is prime by Lemma 3.1 it is sufficient to find the number of nonequivalent MRS with support $\{1, 2, m, r\}$. For that purpose, we fix $3 \leq j < k \leq p$ and look at possible $3 \leq m < r \leq p$ such that $\{1, 2, j, k\} \sim \{1, 2, m, r\}$. Solving the corresponding systems we obtain the following 12 putative values of $\{m, r\}$ (unordered pairs):

$$\begin{aligned}
&\{j,k\}; \{3-j, 3-k\}; \left\{1+(j-1)^{-1}, 1+(k-1)(j-1)^{-1}\right\};\\
&\left\{1+(k-1)^{-1}, 1+(j-1)(k-1)^{-1}\right\}; \left\{2-(j-1)^{-1}, 2-(k-1)(j-1)^{-1}\right\};\\
&\left\{2-(k-1)^{-1}, 2-(j-1)(k-1)^{-1}\right\}; \{1-(j-2)^{-1}, 1+(k-2)(j-2)^{-1}\};\\
&\left\{1-(k-2)^{-1}, 1+(j-2)(k-2)^{-1}\right\}; \{2+(j-2)^{-1}, 2-(k-2)(j-2)^{-1}\};
\end{aligned} \tag{2}$$

$\{2+(k-2)^{-1}, 2-(j-2)(k-2)^{-1}\}; \{1-(j-1)(k-j)^{-1}, 1-(j-2)(k-j)^{-1}\};$
$\{1+(k-1)(k-j)^{-1}, 1+(k-2)(k-j)^{-1}\};$

Case 1. Let $k = j+1, 3 \leq j \leq p-1$. Then the possible values Mod p for $\{m, r\}$ are:

$\{j, j+1\}; \{3-j, 2-j\}; \{1+(j-1)^{-1}, 2+(j-1)^{-1}\}; \{1+j^{-1}, 2-j^{-1}\};$
$\{2-(j-1)^{-1}, 1-(j-1)^{-1}\}; \{2-j^{-1}, 1+j^{-1}\};$
$\{1-(j-2)^{-1}, 2+(j-2)^{-1}\}; \{1-(j-1)^{-1}, 2-(j-1)^{-1}\};$
$\{2+(j-2)^{-1}, 1-(j-2)^{-1}\}; \{2+(j-1)^{-1}, 1+(j-1)^{-1}\};$
$\{2-j, 3-j\}; \{1+j, j\},$

and removing the obvious duplications, we get

$\{j, j+1\}; \{3-j, 2-j\}; \{1+(j-1)^{-1}, 2+(j-1)^{-1}\}; \{1+j^{-1}, 2-j^{-1}\};$
$\{2-(j-1)^{-1}, 1-(j-1)^{-1}\}; \{1-(j-2)^{-1}, 2+(j-2)^{-1}\}.$

(Observe that four pairs of consecutive indices are contained in each such class.)

If $p \equiv 1, 5 \pmod{12}$, by Gauss' reciprocity law, -1 is a quadratic residue modulo p, and so, for $j = 1 \pm (-1)^{1/2}$ Mod p (which happens when $j = 1-(j-1)^{-1}$, for example), the above set of possible values for $\{m, r\}$ shrinks to

$$\{j, j+1\}; \{3-j, 2-j\}; \{1+j^{-1}, 2-j^{-1}\}.$$

Certainly, if $j_1 = 1+(-1)^{1/2}, j_2 = 1-(-1)^{1/2}$, then the class of $\{1, 2, j_1, j_1+1\}$ is the same as the class of $\{1, 2, j_1, j_2+1\}$. (Observe that two pairs of consecutive indices are contained in each such class.)

The contributions to $E(p)_{(\cdot)}$ in all these cases are

$$\begin{aligned} E(p)_{1,5} &\leftarrow 1 + \frac{p-5}{4} = \frac{p-1}{4} \\ E(p)_{7,11} &\leftarrow \frac{p-3}{4} \end{aligned} \tag{3}$$

Case 2. Assume $k \neq j+1$ (of course, by symmetry, nor $j \neq k+1$). If $p \equiv 1, 7 \pmod{12}$, then -3 is a quadratic residue modulo p. For $\{j, k\} = \{(9 \pm (-3)^{1/2})6^{-1}, (3 \pm (-3)^{1/2})2^{-1}\}$ Mod p (these values are obtained by solving the system $3-j = 1+(j-1)(k-1)^{-1}, 3-k = 1+(k-1)^{-1}$, for

example), the set (2) shrinks into a set of 4 elements

$$\begin{aligned}&\{j,k\};\{3-j,3-k\};\\&\left\{1+(j-1)^{-1},1+(k-1)(j-1)^{-1}\right\};\\&\left\{2-(j-1)^{-1},2-(k-1)(j-1)^{-1}\right\}.\end{aligned}$$

In all the other cases when $k \neq j+1$, $j \neq k+1$, either they all belong to the above class, or the cardinality of the set (2) is 12.

The contributions to both $E(p)_1, E(p)_7$ in this last case is

$$1. \tag{4}$$

Putting together (3) and (4) we obtain

$$\begin{aligned}E(p)_1 &= \frac{p-1}{4}+1+\frac{\binom{p-2}{2}-3-4-6\frac{p-5}{4}}{12}=\frac{p^2-2p+25}{24}\\E(p)_5 &= \frac{p-1}{4}+\frac{\binom{p-2}{2}-3-6\frac{p-5}{4}}{12}=\frac{p^2-2p+9}{24}\\E(p)_7 &= \frac{p-3}{4}+1+\frac{\binom{p-2}{2}-4-6\frac{p-3}{4}}{12}=\frac{p^2-2p+13}{24}\\E(p)_{11} &= \frac{p-3}{4}+\frac{\binom{p-2}{2}-6\frac{p-3}{4}}{12}=\frac{p^2-2p-3}{24},\end{aligned}$$

which proves our theorem. □

4. Counting quartic equivalence classes for prime power dimensions

We will now count the S-equivalence classes for quartics in p^ℓ variables ($\ell \geq 2$), where $p \geq 29$ is a prime number. We start with a few lemmas.

Lemma 4.1. *Let f be a quartic MRS in p^ℓ ($\ell \geq 2$) dimension whose support includes $\{1,2,j,k\}$, where $k = j+1$ and $p|(j-1)$, or $p|(j-2)$, or $\gcd(j-1,p) = \gcd(j-2,p) = 1$. Then its equivalence class contains an MRS whose support is $\{1,2,j',k'\}$ where $j'+k' \equiv 3 \pmod{p^\ell}$. Furthermore, the class containing $\{1,2,j,k\}$ with $j+k \equiv 3 \pmod{p^\ell}$ will not contain a class of support $\{1,2,j',k'\}$ with $\gcd(k'-1,p) = \gcd(k'-2,p) = \gcd(j'-1,p) = \gcd(j'-2,p) = \gcd(k'-j',p) = 1$, $|k'-j'| \neq 1$.*

Proof. If $p|(j-1)$ we take the affine transformation of Theorem 2.2 based upon $u = (j-2)^{-1}, v = 1-2(j-2)^{-1}$ and $\{j',k'\} = \{1-(j-2)^{-1}, 2+(j-$

$2)^{-1}\}$ (thus, $j'+k' \equiv 3 \pmod{p^\ell}$; we also note that $p|(j'-1)$ and $p|(k'-2)$, or $p|(j'-2)$ and $p|(k'-1)$). For the second claim, that is, if $p|(j-2)$, we take the affine transformation based upon $u = -j^{-1}, v = 2 + j^{-1}$ and $\{j', k'\} = \{2 - j^{-1}, 1 + j^{-1}\}$ (thus, $j' + k' \equiv 3 \pmod{p^\ell}$). If $p \not|(j-1)$, $p \not|(j-2)$, then either of the two above transformations will do the trick.

The last claim follows easily by solving the corresponding system and analyzing each of the twelve solutions. Since we have done several such and will do more later, we leave this as a warm-up exercise for the reader. □

Lemma 4.2. *Let f be a quartic MRS in p^ℓ ($\ell \geq 2$) dimension, whose support includes $\{1, 2, j, k\}$, where p divides one of $(j-1), (j-2)$, and $\gcd(k-1, p) = \gcd(k-2, p) = 1$; or, p divides one of $(k-1), (k-2)$, and $\gcd(j-1, p) = \gcd(j-2, p) = 1$; or p divides both $(j-1), (k-1)$; or p divides both $(j-2), (k-2)$. Then its class contains an MRS with support $\{1, 2, j', k'\}$ where $p|(k'-j')$ and $\gcd(k'-1, p) = \gcd(k'-2, p) = \gcd(j'-1, p) = \gcd(j'-2, p) = 1$.*

Proof. If $p|(j-2)$ and $\gcd(k-1, p) = \gcd(k-2, p) = 1$, we can use the affine transformation based on $u = (k-1)^{-1}, v = 1-(k-1)^{-1}$, so $\{j', k'\} = \{k(k-1)^{-1}, 1+(j-1)(k-1)^{-1}\}$; if $p|(k-2)$ and $\gcd(j-1, p) = \gcd(j-2, p) = 1$, we can use the affine transformation based on $u = (j-1)^{-1}, v = 1-(j-1)^{-1}$, so $\{j', k'\} = \{j(j-1)^{-1}, 1 + (k-1)(j-1)^{-1}\}$; if $p|(j-1)$ and $\gcd(k-1, p) = \gcd(k-2, p) = 1$, we can use the affine transformation based on $u = (k-2)^{-1}, v = 1 - 2(k-2)^{-1}$, so $\{j', k'\} = \{1 - (k-2)^{-1}, 1 + (j-2)(k-2)^{-1}\}$; if $p|(k-1)$ and $\gcd(j-1, p) = \gcd(j-2, p) = 1$, we can use the affine transformation based on $u = (j-2)^{-1}, v = 1 - 2(j-2)^{-1}$, so $\{j', k'\} = \{1 - (j-2)^{-1}, 1 + (k-2)(j-2)^{-1}\}$. The lemma is shown. □

Remark 4.3. *If $p \not|B = A + 1$ (similarly, for $p \not|A = B + 1$) then $\{1, p^s + 1, Ap^s + 1, Bp^s + 1\} \sim \{1, p^s + 1, ap^s + 1, bp^s + 1\}$ with $a + b \equiv 1 \pmod{p^{\ell-s}}$ (use the transformation based on $u = -(A+1)^{-1}, v = 1-(A+1)^{-1}$, $a = 1-(A+1)^{-1}, b = (1-a)$ Mod $p^{\ell-s}$). Also, $p \not|(a-1)b$, and if $p \not|(A-1)A(A+1)$, then $p \not|ab(a-1)(b-1)$.*

Theorem 4.4. *Let $p \geq 29$ be a prime. Then the number of S-equivalence*

classes of quartic MRS in p^ℓ variables ($\ell \geq 2$) is

$$E(p^\ell)_1 = \frac{p^{2\ell+2} + p^{2\ell+1} + p^{2\ell} - 3p^{\ell+2} - 6p^{\ell+1} - 3p^\ell + p^2(27\ell+2) + 5p - 27\ell + 2}{24\,(p^2-1)}$$
$$E(p^\ell)_5 = \frac{p^{2\ell+2} + p^{2\ell+1} + p^{2\ell} - 3p^{\ell+2} - 6p^{\ell+1} - 3p^\ell + p^2(11\ell+2) + 5p - 11\ell + 2}{24\,(p^2-1)}$$
$$E(p^\ell)_7 = \frac{p^{2\ell+2} + p^{2\ell+1} + p^{2\ell} - 3p^{\ell+2} - 6p^{\ell+1} - 3p^\ell + p^2(15\ell+2) + 5p - 15\ell + 2}{24\,(p^2-1)}$$
$$E(p^\ell)_{11} = \frac{p^{2\ell+2} + p^{2\ell+1} + p^{2\ell} - 3p^{\ell+2} - 6p^{\ell+1} - 3p^\ell - p^2(\ell-2) + 5p + \ell + 2}{24\,(p^2-1)}.$$

Proof. By Lemma 3.1, to count the number of equivalence classes of quartics in p^ℓ dimension, it will be sufficient to count the classes with support $\{1,2,j,k\}$ with $3 \leq j, bk \leq p^\ell$, and also count classes with support $\{1, p^s+1, ap^s+1, bp^s+1\}$, $\gcd(ab,p)=1$, $1 \leq s \leq \ell-1$, or $p|\gcd(a,b-1)$ (or $p|\gcd(b,a-1)$), $2 \leq a,b \leq p^{\ell-s}-1$.

Case *A*. First, given a class with support $\{1,2,j,k\}$, the only possible values for $\{m,r\}$ with $\{1,2,j,k\} \sim \{1,2,m,r\}$ are listed in (2). We consider several subcases.

Subcase (A_1). $k+j \equiv 3 \pmod{p^\ell}$ (of course, $j \neq k$). We get the following possibilities (removing the obvious duplications) for $\{m,r\}$ where $\{1,2,j,k\} \sim \{1,2,m,r\}$:

$$\{j, 3-j\}; \{(j-1)^{-1}, 1+(j-1)^{-1}\}; \{-(j-2)^{-1}, 1-(j-2)^{-1}\};$$
$$\{2-(j-1)^{-1}, 3-(j-1)^{-1}\}; \{2+(j-2)^{-1}, 3+(j-2)^{-1}\};$$
$$\{\left(3-(2j-3)^{-1}\right)2^{-1}, \left(3+(2j-3)^{-1}\right)2^{-1}\}.$$

(Observe that $2j-3$ is invertible, unless $j \equiv 1+2^{-1} \equiv \frac{p^\ell+3}{2} \pmod{p}$; also, $j \not\equiv \frac{p^\ell+3}{2} \pmod{p^\ell}$, since then $j = 3-j$ Mod p^ℓ, which is impossible.)

It is straightforward to check that there are exactly two pairs $\{m,r\}$ in the above list satisfying $m+r \equiv 3 \pmod{p^\ell}$, namely the first and the last ones, except when $j \equiv \frac{p^\ell+3}{2} \pmod{p}$, or when $p \equiv 1,5 \pmod{12}$ (since, by Gauss' reciprocity law, -1 is a quadratic residue modulo p) and so, for $j = (3 \pm (-1)^{1/2})2^{-1}$ Mod p the two pairs overlap (precisely, $j = \left(3-(2j-3)^{-1}\right)2^{-1}$ and $3-j = \left(3+(2j-3)^{-1}\right)2^{-1}$). It is obvious that there are $\frac{p^\ell-3}{2}$ ordered pairs (j,k) $(j,k \geq 3)$ with $k+j \equiv 3 \pmod{p^\ell}$ out of which $\frac{p^{\ell-1}-1}{2}$ of them satisfy $j \equiv \frac{p^\ell+3}{2} \pmod{p}$.

Thus, the contribution to $E(p^\ell)_{(\cdot)}$ in this case is

$$\begin{aligned} E(p^\ell)_{1,5} &\longleftarrow 1+\frac{p^{\ell-1}-1}{2}+\frac{1}{2}\left(\frac{p^\ell-3}{2}-1-\frac{p^{\ell-1}-1}{2}\right)=\frac{p^\ell+p^{\ell-1}-2}{4}, \\ E(p^\ell)_{7,11} &\longleftarrow \frac{p^{\ell-1}-1}{2}+\frac{1}{2}\left(\frac{p^\ell-3}{2}-\frac{p^{\ell-1}-1}{2}\right)=\frac{p^\ell+p^{\ell-1}-4}{4}. \end{aligned} \tag{5}$$

Subcase (A_2). $k+j \not\equiv 3 \pmod{p^\ell}$, $p|(k-j)$, and $\gcd(k-1,p)=\gcd(k-2,p)=\gcd(j-1,p)=\gcd(j-2,p)=1$, or $p|\gcd(j-1,k-1)$, or $p|\gcd(j-2,k-2)$. We get the following possibilities for $\{m,r\}$ where $\{1,2,j,k\}\sim\{1,2,m,r\}$:

for $\gcd(k-1,p)=\gcd(k-2,p)=\gcd(j-1,p)=\gcd(j-2,p)=1$:
$\{j,k\};\{3-j,3-k\};\left\{1+(j-1)^{-1},1+(k-1)(j-1)^{-1}\right\};$
$\left\{1+(k-1)^{-1},1+(j-1)(k-1)^{-1}\right\};\left\{2-(j-1)^{-1},2-(k-1)(j-1)^{-1}\right\};$
$\left\{2-(k-1)^{-1},2-(j-1)(k-1)^{-1}\right\};\{1-(j-2)^{-1},1+(k-2)(j-2)^{-1}\};$
$\left\{1-(k-2)^{-1},1+(j-2)(k-2)^{-1}\right\};\{2+(j-2)^{-1},2-(k-2)(j-2)^{-1}\};$
$\left\{2+(k-2)^{-1},2-(j-2)(k-2)^{-1}\right\},$

and

for $p|(j-1)$ and $p|(k-1)$:
$\{j,k\};\{3-j,3-k\};\{1-(j-2)^{-1},1+(k-2)(j-2)^{-1}\};$
$\left\{1-(k-2)^{-1},1+(j-2)(k-2)^{-1}\right\};\{2+(j-2)^{-1},2-(k-2)(j-2)^{-1}\};$
$\left\{2+(k-2)^{-1},2-(j-2)(k-2)^{-1}\right\},$
for $p|(j-2)$ and $p|(k-2)$:
$\{j,k\};\{3-j,3-k\};\left\{1+(j-1)^{-1},1+(k-1)(j-1)^{-1}\right\};$
$\left\{1+(k-1)^{-1},1+(j-1)(k-1)^{-1}\right\};\left\{2-(j-1)^{-1},2-(k-1)(j-1)^{-1}\right\};$
$\left\{2-(k-1)^{-1},2-(j-1)(k-1)^{-1}\right\}.$

We observe that the last two possibilities are not different since, if $p|(k-1)$ and $p|(j-1)$, then the class of $\{1,2,j,k\}$ will contain $\{1,2,j',k'\}$ with $p|(k'-2), p|(j'-2)$ (for example, $\{j',k'\}:=\{3-j,3-k\}$), and viceversa. Moreover, there are exactly two pairs in each class satisfying the required conditions; for example, if $p|(j-1), p|(k-1)$, then in the class of $\{1,2,j,k\}$ one can find only two others $\{1,2,j',k\}$ with $p|(j'-1), p|(k'-1)$, namely, $\{j',k'\}=\{2+(j-2)^{-1},2-(k-2)(j-2)^{-1}\}$ and $\{j',k'\}=\{2+(k-2)^{-1},2-(j-2)(k-2)^{-1}\}$.

Summarizing, every class in the first category ($\gcd(k-1,p)=\gcd(k-2,p)=\gcd(j-1,p)=\gcd(j-2,p)=1$) contains only two pairs (recall that $j+k\not\equiv 3 \pmod{p^\ell}$, as in that case we would have only one pair), satisfying

the imposed conditions, and every class in the second category ($p|(j-1)$ and $p|(k-1)$, or $p|(j-2)$ and $p|(k-2)$) contains exactly three pairs satisfying the imposed conditions.

There are $\frac{(p^{\ell-1}-1)(p^{\ell-1}-2)}{2}$ ordered pairs (j,k) satisfying $p|(j-1), p|(k-1)$ and the same number satisfying $p|(j-2), p|(k-2)$. There are $\frac{(p^{\ell-1}-1)(p^{\ell}-4)}{2}$ ordered pairs (j,k) with $p|(k-j)$, from which we take away the ones satisfying $p|(j-1)$ and $p|(k-1)$, or $p|(j-2)$ and $p|(k-2)$, or $j+k\equiv 3 \pmod{p^\ell}$. Using an inclusion-exclusion easy argument, we obtain

$$\begin{aligned}&\frac{\left(p^{\ell-1}-1\right)\left(p^{\ell}-4\right)}{2}-2\frac{(p^{\ell-1}-1)(p^{\ell-1}-2)}{2}-\frac{p^{\ell-1}-2}{2}\\&=\frac{(p^{\ell-1}-1)(p^{\ell}-2p^{\ell-1}-1)}{2}\end{aligned}$$

number of pairs (j,k) with $p|(k-j)\neq 0$ and $j+k\not\equiv 3 \pmod{p^\ell}$ such that $\gcd(k-1,p)=\gcd(k-2,p)=\gcd(j-1,p)=\gcd(j-2,p)=1$.

Thus, the contribution to $E(p^\ell)_{(.)}$ in this case is

$$\begin{aligned}E(p^\ell)_{1,5,7,11} \longleftarrow &\frac{1}{2}\frac{(p^{\ell-1}-1)(p^{\ell}-2p^{\ell-1}-1)}{2}+\frac{1}{3}\frac{(p^{\ell-1}-1)(p^{\ell-1}-2)}{2}\\&=\frac{(p^{\ell-1}-1)(3p^{\ell}-4p^{\ell-1}-7)}{12}.\end{aligned}\tag{6}$$

Subcase (A_3). $j+k\not\equiv 3 \pmod{p^\ell}$, $|j-k|\neq 1$, and $p|(k-1)$ and $p|(j-2)$, or, $p|(k-2)$ and $p|(j-1)$ (thus, $p\not|(k-j)$). The possible values for $\{m,r\}$ with $\{1,2,j,k\}\sim\{1,2,m,r\}$ are (all different Mod p^ℓ):

for $p|(k-2)$ and $p|(j-1)$:
$\{j,k\};\{3-j,3-k\};\left\{1+(k-1)^{-1},1+(j-1)(k-1)^{-1}\right\};$
$\left\{2-(k-1)^{-1},2-(j-1)(k-1)^{-1}\right\};\{1-(j-2)^{-1},1+(k-2)(j-2)^{-1}\};$
$\{2+(j-2)^{-1},2-(k-2)(j-2)^{-1}\};\left\{1-(j-1)(k-j)^{-1},1-(j-2)(k-j)^{-1}\right\};$
$\left\{1+(k-1)(k-j)^{-1},1+(k-2)(k-j)^{-1}\right\}.$
for $p|(k-1)$ and $p|(j-2)$:
$\{j,k\};\{3-j,3-k\};\left\{1+(j-1)^{-1},1+(k-1)(j-1)^{-1}\right\};$
$\left\{2-(j-1)^{-1},2-(k-1)(j-1)^{-1}\right\};\left\{1-(k-2)^{-1},1+(j-2)(k-2)^{-1}\right\};$
$\left\{2+(k-2)^{-1},2-(j-2)(k-2)^{-1}\right\};\left\{1-(j-1)(k-j)^{-1},1-(j-2)(k-j)^{-1}\right\};$
$\left\{1+(k-1)(k-j)^{-1},1+(k-2)(k-j)^{-1}\right\}.$

We observe that the two possibilities are not different since, if $p|(k-1)$ and $p|(j-2)$, then the class of $\{1,2,j,k\}$ will contain $\{1,2,j',k'\}$ with

$p|(k'-2), p|(j'-1)$ (for example, $k' := 1+(j-1)^{-1}$, $j' := 1+(k-1)(j-1)^{-1}$), and viceversa. Moreover, every pair $\{j',k'\}$ in the class of $\{j,k\}$ with $p|(k-1)$ and $p|(j-2)$ satisfies the same condition (for some choice of j',k'): for example, for $\left\{k' := 1+(k-1)^{-1}, j' := 1+(j-1)(k-1)^{-1}\right\}$, we have $p|(j'-2), p|(k'-1)$.

The number of pairs $\{j,k\}$ $(j,k \geq 3,\ |j-k| \neq 1)$ with $p|(k-2)$ and $p|(j-1)$ and $k+j \not\equiv 3 \pmod{p^\ell}$ is exactly $(p^{\ell-1}-1)(p^{\ell-1}-3)$. Thus, the contribution to $E(p^\ell)_{(\cdot)}$ in this case is

$$E(p^\ell)_{1,5,7,11} \longleftarrow \frac{(p^{\ell-1}-1)(p^{\ell-1}-3)}{8}. \tag{7}$$

Subcase (A_4). $k+j \not\equiv 3 \pmod{p^\ell}$, $\gcd(k-1,p) = \gcd(k-2,p) = \gcd(j-1,p) = \gcd(j-2,p) = \gcd(k-j,p) = 1$, as well as $|k-j| \neq 1$ $(j,k \geq 3)$. The possible values for $\{m,r\}$ Mod p^ℓ with $\{1,2,j,k\} \sim \{1,2,m,r\}$ are as in (2). As before, if $p \equiv 1,7 \pmod{12}$, then -3 is a quadratic residue modulo p; for $\{j,k\} = \{(9 \pm (-3)^{1/2})6^{-1}, (3 \pm (-3)^{1/2})2^{-1}\}$ Mod p^ℓ (or, $\{j,k\} = \{(5 \pm (-3)^{1/2})2^{-1}, (5 \mp (-3)^{1/2})2^{-1}\}$, etc.), the set (2) of values for $\{m,r\}$ shrinks into the same set of four elements

$$\begin{aligned}&\{j,k\}; \{3-j,3-k\}; \left\{1+(j-1)^{-1}, 1+(k-1)(j-1)^{-1}\right\};\\ &\left\{2-(j-1)^{-1}, 2-(k-1)(j-1)^{-1}\right\}.\end{aligned}$$

Since we often use the inclusion–exclusion principle in the paper (in the "underground") we will display explicitly such a use of the it to count the number of *ordered* pairs with the above conditions (we always assume that $3 \leq j < k \leq p^\ell$).

Let $X_1 = \{(j,k) \,|\, |k-j| \neq 1, k+j \equiv 3 \pmod{p^\ell}\}$, $X_2 = \{(j,k) \,|\, |k-j| \neq 1, p|k-1, or\ p|k-2\}$, $X_3 = \{(j,k) \,|\, |k-j| \neq 1, p|j-1, or\ p|j-2\}$, $X_4 = \{(j,k) \,|\, |k-j| \neq 1, p|k-j\}$. We see that

$$|X_1| = \frac{p^\ell-3}{2}, |X_2| = |X_3| = (p^\ell-5)(p^{\ell-1}-1), |X_4| = \frac{(p^\ell-4)(p^{\ell-1}-1)}{2}$$

(the last count is obtained, by observing that for every $j \geq 3$, we let $k = ap+j$, where $1 \leq a \leq p^{\ell-1}-j/p$, and so, $|X_4| = \sum_{i=1}^{p^{\ell-1}-1} p(p^{\ell-1}-i) - 2(p^{\ell-1}-1)$, which simplifies to the above expression). Observe that the universal set $S = \{(j,k) \,|\, k > j+1 \geq 4\}$ has $|S| = \binom{p^\ell-2}{2} - (p^\ell-3)$ (to account for

$k = j + 1$). Further,

$$
\begin{aligned}
&|X_1 \cap X_2| = p^{\ell-1} - 1; |X_1 \cap X_3| = p^{\ell-1} - 1;\\
&|X_1 \cap X_4| = \frac{p^{\ell-1} - 1}{2}; |X_2 \cap X_3| = 2(p^{\ell-1} - 1)(p^{\ell-1} - 2);\\
&|X_2 \cap X_4| = (p^{\ell-1} - 1)(p^{\ell-1} - 2); |X_3 \cap X_4| = (p^{\ell-1} - 1)(p^{\ell-1} - 2);\\
&|X_1 \cap X_2 \cap X_3| = p^{\ell-1} - 1; |X_1 \cap X_2 \cap X_4| = 0;\\
&|X_1 \cap X_3 \cap X_4| = 0; |X_2 \cap X_3 \cap X_4| = (p^{\ell-1} - 1)(p^{\ell-1} - 2);\\
&|X_1 \cap X_2 \cap X_3 \cap X_4| = 0.
\end{aligned}
$$

Using the complementary form of the inclusion–exclusion principle for $N = 4$ sets in the universal set S we introduced earlier, we obtain

$$
\begin{aligned}
\left|\bigcap_{i=1}^{4} \overline{X_i}\right| &= |S| - \sum_{i=1}^{N} |X_i| + \sum_{1 \le i < j \le N} |X_i \cap X_j| - \cdots + (-1)^n |X_1 \cap \ldots \cap X_N|\\
&= \binom{p^\ell - 2}{2} - \frac{3(p^\ell - 3)}{2} - 2(p^\ell - 5)(p^{\ell-1} - 1) - \frac{(p^\ell - 4)(p^{\ell-1} - 1)}{2}\\
&+ \frac{3(p^\ell - 1)}{2} + 3(p^{\ell-1} - 1)(p^{\ell-1} - 2)\\
&= \frac{p^{2\ell} - 5p^{2\ell-1} + 6p^{2\ell-2} - 3p^\ell + 9p^{\ell-1}}{2} = \frac{p^{\ell-1}(p^\ell - 2p^{\ell-1} - 3)(p-3)}{2}.
\end{aligned}
$$

Thus, the contribution to $E(p^\ell)_{(\cdot)}$ in this case is

$$
\begin{aligned}
E(p^\ell)_{1,7} &\longleftarrow 1 + \frac{p^{\ell-1}(p^\ell - 2p^{\ell-1} - 3)(p-3)}{24} - \frac{1}{3},\\
E(p^\ell)_{5,11} &\longleftarrow \frac{p^{\ell-1}(p^\ell - 2p^{\ell-1} - 3)(p-3)}{24}.
\end{aligned}
\tag{8}
$$

Case B. Next, fix $1 \le s \le \ell - 1$ and consider a class of support $\{1, p^s + 1, ap^s+1, bp^s+1\}$, $\gcd(ab, p) = 1$ (with p dividing either both of $(a-1)$, $(b-1)$, or none). We consider separately the two subcases (these are disjoint, as one can see from the proof of Lemma 3.1). (To simplify our counts a bit, we assume that all the expressions are reduced modulo $p^{\ell-s}$, because $ap^s + 1$ is the same index as $(a + p^{\ell-s})p^s + 1$ Mod p^ℓ.) By abuse of notation, if $\{1, p^s + 1, ap^s + 1, bp^s + 1\} \sim \{1, p^s + 1, mp^s + 1, rp^s + 1\}$, then we say that $\{a, b\}$, $\{m, r\}$ are equivalent and often write $\{a, b\} \sim \{m, r\}$.

Subcase (B_1). $p \not| ab$, $p|(a-1)$ and $p|(b-1)$. The potential values of $\{m, r\} \sim$

$\{a,b\}$ Mod $p^{\ell-s}$ are

$$\{a,b\};\{1-a,1-b\};\{a^{-1},ba^{-1}\};\{b^{-1},ab^{-1}\};$$
$$\{1-a^{-1},1-ba^{-1}\};\{1-b^{-1},1-ab^{-1}\}.$$

(We make here an observation, which we will use later: all six values $\{m,r\}$ above satisfy the property that $p|(m-r)$.) Removing the above pairs that do not obviously satisfy the conditions $p|(a-1), p|(b-1)$ we get the potential values (all distinct Mod $p^{\ell-s}$):

$$\{a,b\};\{a^{-1},ba^{-1}\};\{b^{-1},ab^{-1}\}.$$

For a fixed s, there are $\frac{(p^{\ell-s-1}-1)(p^{\ell-s-1}-2)}{2}$ ordered pairs (a,b) with $p|\gcd(a-1,b-1)$, and so, summing them over $1\le s\le \ell-1$, we obtain that the contribution to $E(p^\ell)_{(\cdot)}$ in this subcase is

$$\begin{aligned} E(p^\ell)_{1,5,7,11} &\longleftarrow \frac{p^{2\ell-2}-3p^\ell-3p^{\ell-1}+2(\ell-1)p^2-2(\ell-2)+3p}{6\,(p^2-1)} \\ &= \frac{(p^{\ell-1}-1)(p^{\ell-1}-3p-2)}{6\,(p^2-1)}+\frac{\ell-1}{3}. \end{aligned} \tag{9}$$

Using the above observation, there are $\frac{(p^{\ell-1}-1)(p^{\ell-1}-3p-2)}{2(p^2-1)}+\ell-1$ pairs (a,b) with $p|(a-b)$ and $p\not|(a-1)(b-1)$ (since for all, p divides both a,b) contained in all of these classes, which we have to disregard later.

Subcase (B_2). $p\not|ab(a-1)(b-1)$, $p|(a-b)$, $a+b\not\equiv 1 \pmod{p^{\ell-s}}$. The ten potential values Mod p^ℓ of $\{a,b\}$ are (all distinct)

$$\{a,b\};\{1-a,1-b\};\{a^{-1},ba^{-1}\};\{b^{-1},ab^{-1}\};$$
$$\{1-a^{-1},1-ba^{-1}\};\{1-b^{-1},1-ab^{-1}\};$$
$$\{-(a-1)^{-1},(b-1)(a-1)^{-1}\};\{-(b-1)^{-1},(a-1)(b-1)^{-1}\};$$
$$\{1+(a-1)^{-1},1-(b-1)(a-1)^{-1}\};\{1+(b-1)^{-1},1-(a-1)(b-1)^{-1}\}.$$

We observe that in the above list there are only two pairs that fully satisfy the imposed conditions. An elementary inclusion–exclusion argument shows that there are $\frac{(p^{\ell-s-1}-1)(p^{\ell-s}-2p^{\ell-s-1}-1)}{2}$ for which $p|(a-b)$, $a+b\not\equiv 1 \pmod{p^{\ell-s}}$, $p\not|ab(a-1)(b-1)$. Summing over $1\le s\le \ell-1$, we obtain a total of $\frac{p^{2\ell-1}-2p^{2\ell-2}-p^{\ell+1}+p^{\ell-1}-p+2}{2(p^2-1)}+\frac{\ell}{2}$ such pairs. The contribution to

$E(p^\ell)_{(\cdot)}$ in this case is

$$\begin{aligned} E(p^\ell)_{1,5,7,11} &= \frac{p^{2\ell-1} - 2p^{2\ell-2} - p^{\ell+1} + p^{\ell-1} - p + 2}{4(p^2-1)} + \frac{\ell}{4} \\ &= \frac{(p^{2\ell-2}-1)(p-2)}{4(p^2-1)} - \frac{p^{\ell-1}-\ell}{4}. \end{aligned} \tag{10}$$

Subcase (B_3). $p \not| ab(a-1)(b-1)(a-b)$, $a+b \not\equiv 1 \pmod{p^{\ell-s}}$. If $|a-b|=1$, say $b=a+1$, there exists a representative based on a', b' in the same class, satisfying the conditions $p \not| a'b'(a'-1)(b'-1)(a'-b')$ along with $|a'-b'|>1$ (use transformation $u=b^{-1}, v=1-b^{-1}$, $a'=b^{-1}, b'=ab^{-1}$). Thus, we will assume that $|a-b|>1$.

The potential values of $\{m,r\}$ Mod p^ℓ, where $\{1, p^s+1, ap^s+1, bp^s+1\} \sim \{1, p^s+1, mp^s+1, rp^s+1\}$ (observe that $2 \le a, b \le p^{\ell-s}$) are:

$$\begin{aligned} &\{a,b\}; \{1-a, 1-b\}; \{a^{-1}, ba^{-1}\}; \{b^{-1}, ab^{-1}\}; \{1-a^{-1}, 1-ba^{-1}\}; \\ &\{1-b^{-1}, 1-ab^{-1}\}; \{-(a-1)^{-1}, (b-1)(a-1)^{-1}\}; \{-(b-1)^{-1}, (a-1)(b-1)^{-1}\}; \\ &\{1+(a-1)^{-1}, 1-(b-1)(a-1)^{-1}\}; \{1+(b-1)^{-1}, 1-(a-1)(b-1)^{-1}\}; \\ &\{a(a-b)^{-1}, (a-1)(a-b)^{-1}\}; \{b(b-a)^{-1}, (b-1)(b-a)^{-1}\}. \end{aligned} \tag{11}$$

If $p \equiv 1, 7 \pmod{12}$, then there exist two (nontrivial) cubic roots a, b of 1 (this is equivalent to $p^\ell \,|\, a^2+a+1$, $p^\ell \,|\, b^2+b+1$; we also note that the two cubic roots satisfy $a+b+1 \equiv 0 \pmod{p^{\ell-s}}$). For these two values (they occur when the first and fourth pairs in (11) are the same), of course, reduced modulo $p^{\ell-s}$, the set (11) shrinks into a four element set

$$\{a,b\}; \{1-a, 1-b\}; \{-(a-1)^{-1}, (b-1)(a-1)^{-1}\}; \{-(b-1)^{-1}, (a-1)(b-1)^{-1}\}.$$

In all the other cases, the set (11) has 12 distinct elements.

Yet another inclusion–exclusion argument reveals that there are $n_s := \frac{p^{\ell-s-1}(p^{\ell-s}-2p^{\ell-s-1}-3)(p-3)}{2}$ ordered pairs (a,b) with $p \not| ab(a-1)(b-1)(a-b)$ and $|a-b| \ne 1$, $a+b \not\equiv 1 \pmod{p^{\ell-s}}$. Summing over $1 \le s \le \ell-1$, we obtain a total of $\frac{(p-3)(p^{2\ell-1}-2p^{2\ell-2}-3p^\ell-3p^{\ell-1}+2p+5)}{2(p^2-1)}$ such pairs. For $p \equiv 1, 7 \pmod{12}$, we sum $n_s - 4$ for every s, to account for the pairs in the class of the mentioned cubic roots.

The contribution to $E(p^\ell)_{(\cdot)}$ in this case is

$$\begin{aligned} E(p^\ell)_{1,7} &\longleftarrow (\ell-1) + \frac{(p-3)\left(p^{2\ell-1} - 2p^{2\ell-2} - 3p^\ell - 3p^{\ell-1} + 2p + 5\right)}{24(p^2-1)} - \frac{4(\ell-1)}{12}, \\ E(p^\ell)_{5,11} &\longleftarrow \frac{(p-3)\left(p^{2\ell-1} - 2p^{2\ell-2} - 3p^\ell - 3p^{\ell-1} + 2p + 5\right)}{24(p^2-1)}. \end{aligned} \tag{12}$$

Subcase (B_4). $p \not| ab(a-1)(b-1)$, $p|(a-b)$, $a+b \equiv 1 \pmod{p^{\ell-s}}$. The set (11) contracts into the 5 element set

$$\{a, 1-a\}; \{-1+a^{-1}, a^{-1}\}; \{-(a-1)^{-1}, -1+(a-1)^{-1}\};$$
$$\{1-a^{-1}, 2-a^{-1}\}; \{1+(a-1)^{-1}, 2+(a-1)^{-1}\}.$$

We note that in the above list, there is only one pair satisfying the imposed conditions, and there are $\frac{p^{\ell-s-1}-1}{2}$ such ordered pairs, which summed for $1 \leq s \leq \ell-1$ gives the contribution to $E(p^\ell)$ in this case

$$E(p^\ell)_{1,5,7,11} \longleftarrow \frac{p(p^{\ell-2}-1)}{2(p-1)} - \frac{\ell-2}{2}. \tag{13}$$

Subcase (B_5). $p \not| ab(a-1)(b-1)(a-b)$, $a+b \equiv 1 \pmod{p^{\ell-s}}$. The set (11) shrinks to six elements, namely

$$\begin{aligned}&\{a, 1-a\}; \{a^{-1}, -1+a^{-1}\}; \{-(a-1)^{-1}, -1-(a-1)^{-1}\}; \{1-a^{-1}, 2-a^{-1}\};\\ &\{1+(a-1)^{-1}, 2+(a-1)^{-1}\}; \{a(2a-1)^{-1}, 1-a(2a-1)^{-1}\}.\end{aligned} \tag{14}$$

We note that only two pairs in the above set satisfy the imposed conditions (the first and the last pairs). If $p \equiv 1, 5 \pmod{12}$, then -1 is a quadratic residue modulo p^ℓ, and for $\{a, b\} = \{1 \pm (-1)^{1/2})2^{-1}\}$ (where $\{a, 1-a\} = \{1-a(2a-1)^{-1}, a(2a-1)^{-1}\}$) the above set shrinks into the same four element set (regardless of the chosen sign)

$$\{a, b\}; \{1-a, 1-b\}; \{a^{-1}, ba^{-1}\}; \{1+(b-1)^{-1}, 1-(a-1)(b-1)^{-1}\}.$$

In all the other cases the set (14) contains distinct elements. There are $m_s := \frac{p^{\ell-s-1}(p-1)}{2}$ pairs satisfying the conditions of this case, which summed over $1 \leq s \leq \ell-1$, gives us a total of $\frac{(p^{\ell-1}-1)(p-3)}{2(p-1)}$ such pairs. For $p \equiv 1, 5 \pmod{12}$ we sum $m_s - 2$ (to account for the pair $\{1 \pm (-1)^{1/2})2^{-1}\}$), for every s.

Thus, the contribution to $E(p^\ell)_{(\cdot)}$ in this case is

$$\begin{aligned}E(p^\ell)_{1,5} &\longleftarrow \frac{(p^{\ell-1}-1)(p-3)}{4(p-1)} + \frac{\ell-1}{2},\\ E(p^\ell)_{7,11} &\longleftarrow \frac{(p^{\ell-1}-1)(p-3)}{4(p-1)}.\end{aligned} \tag{15}$$

Case C. Last, fix $1 \leq s \leq \ell-2$ (of course, this case needs $\ell \geq 3$) and consider a class of support $\{1, p^s+1, ap^{s+1}+1, (bp+1)p^s+1\}$ ($a' := ap, b' := bp+1$).

The 8 potential values of (a,b) Mod $p^{\ell-s-1}$ are (we consider ordered pairs here, since a appears in ap^{s+1}, while b is in $(bp+1)p^s$, so their roles are not interchangeable)

$$\begin{aligned}&(a,b);(-b,-a);(a(bp+1)^{-1},-b(bp+1)^{-1});(b(bp+1)^{-1},-a(bp+1)^{-1});\\&(a(ap-1)^{-1},-b(ap-1)^{-1});(b(ap-1)^{-1},-a(ap-1)^{-1});\\&(-a(bp-ap+1)^{-1},-b(bp-ap+1)^{-1});(b(bp-ap+1)^{-1},a(bp-ap+1)^{-1}).\end{aligned}\tag{16}$$

We note that (assuming order) the set (16) contains either 4 or 8 disjoint elements. We have 4 elements when the class has a representative (a,b) with $a+b\equiv 0 \pmod{p^{\ell-s-1}}$, or $a=b$. The number of such pairs is exactly $2(p^{\ell-s-1}-1)$ (the two conditions do not overlap, since if $a=b$ and $a+b\equiv 0 \pmod{p^{\ell-s-1}}$, then it follows that $p^{\ell-s-1}\,|\,a$, which is impossible). The remaining number of pairs (of class cardinality 8) is exactly $(p^{\ell-s-1}-1)(p^{\ell-s-1}-2)-(p^{\ell-s-1}-1)=p^{2\ell-2s-2}-4p^{\ell-s-1}+3$.

Thus, the contribution to $E(p^\ell)_{(\cdot)}$ of class C is

$$\begin{aligned}E(p^\ell)_{1,5,7,11} &\longleftarrow \sum_{s=1}^{\ell-2}\left(\frac{p^{\ell-s-1}-1}{2}+\frac{p^{2\ell-2s-2}-4p^{\ell-s-1}+3}{8}\right)\\&=\sum_{s=1}^{\ell-2}\frac{p^{2\ell-2s-2}-1}{8}=\frac{p^{2\ell-2}-1}{8(p^2-1)}-\frac{\ell-1}{8}.\end{aligned}\tag{17}$$

Putting together equations (5), (6), (7), (8), (9), (10), (12), (13), (15) and (17), we obtain

$$\begin{aligned}E(p^\ell)_1 &\longleftarrow \frac{p^\ell+p^{\ell-1}-2}{4}+\frac{(p^{\ell-1}-1)(3p^\ell-4p^{\ell-1}-7)}{12}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3)}{8}\\&+1+\frac{p^{\ell-1}(p^\ell-2p^{\ell-1}-3)(p-3)}{24}-\frac{1}{3}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3p-2)}{6\,(p^2-1)}+\frac{\ell-1}{3}\\&+\frac{(p^{2\ell-2}-1)(p-2)}{4(p^2-1)}-\frac{p^{\ell-1}-\ell}{4}+\frac{(p-3)\left(p^{2\ell-1}-2p^{2\ell-2}-3p^\ell-3p^{\ell-1}+2p+5\right)}{24(p^2-1)}\\&+(\ell-1)+\frac{p(p^{\ell-2}-1)}{2(p-1)}-\frac{\ell-2}{2}+\frac{(p^{\ell-1}-1)(p-3)}{4(p-1)}+\frac{\ell-1}{2}+\frac{p^{2\ell-2}-1}{8(p^2-1)}-\frac{\ell-1}{8}\\&=\frac{p^{2\ell+2}+p^{2\ell+1}+p^{2\ell}-3p^{\ell+2}-6p^{\ell+1}-3p^\ell+p^2(27\ell+2)+5p-27\ell+2}{24\,(p^2-1)},\\E(p^\ell)_5 &\longleftarrow \frac{p^\ell+p^{\ell-1}-2}{4}+\frac{(p^{\ell-1}-1)(3p^\ell-4p^{\ell-1}-7)}{12}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3)}{8}\\&+\frac{p^{\ell-1}(p^\ell-2p^{\ell-1}-3)(p-3)}{24}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3p-2)}{6\,(p^2-1)}+\frac{\ell-1}{3}\\&+\frac{(p^{2\ell-2}-1)(p-2)}{4(p^2-1)}-\frac{p^{\ell-1}-\ell}{4}+\frac{(p-3)\left(p^{2\ell-1}-2p^{2\ell-2}-3p^\ell-3p^{\ell-1}+2p+5\right)}{24(p^2-1)}\end{aligned}$$

$$+\frac{p(p^{\ell-2}-1)}{2(p-1)}-\frac{\ell-2}{2}+\frac{(p^{\ell-1}-1)(p-3)}{4(p-1)}+\frac{\ell-1}{2}+\frac{p^{2\ell-2}-1}{8(p^2-1)}-\frac{\ell-1}{8}$$
$$=\frac{p^{2\ell+2}+p^{2\ell+1}+p^{2\ell}-3p^{\ell+2}-6p^{\ell+1}-3p^{\ell}+p^2(11\ell+2)+5p-11\ell+2}{24\,(p^2-1)},$$
$$E(p^{\ell})_7 \longleftarrow \frac{p^{\ell}+p^{\ell-1}-4}{4}+\frac{(p^{\ell-1}-1)(3p^{\ell}-4p^{\ell-1}-7)}{12}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3)}{8}$$
$$+1+\frac{p^{\ell-1}(p^{\ell}-2p^{\ell-1}-3)(p-3)}{24}-\frac{1}{3}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3p-2)}{6\,(p^2-1)}+\frac{\ell-1}{3}$$
$$+\frac{(p^{2\ell-2}-1)(p-2)}{4(p^2-1)}-\frac{p^{\ell-1}-\ell}{4}+\frac{(p-3)\left(p^{2\ell-1}-2p^{2\ell-2}-3p^{\ell}-3p^{\ell-1}+2p+5\right)}{24(p^2-1)}$$
$$+(\ell-1)+\frac{p(p^{\ell-2}-1)}{2(p-1)}-\frac{\ell-2}{2}+\frac{(p^{\ell-1}-1)(p-3)}{4(p-1)}+\frac{p^{2\ell-2}-1}{8(p^2-1)}-\frac{\ell-1}{8}$$
$$=\frac{p^{2\ell+2}+p^{2\ell+1}+p^{2\ell}-3p^{\ell+2}-6p^{\ell+1}-3p^{\ell}+p^2(15\ell+2)+5p-15\ell+2}{24\,(p^2-1)},$$
$$E(p^{\ell})_{11} \longleftarrow \frac{p^{\ell}+p^{\ell-1}-4}{4}+\frac{(p^{\ell-1}-1)(3p^{\ell}-4p^{\ell-1}-7)}{12}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3)}{8}$$
$$+\frac{p^{\ell-1}(p^{\ell}-2p^{\ell-1}-3)(p-3)}{24}+\frac{(p^{\ell-1}-1)(p^{\ell-1}-3p-2)}{6\,(p^2-1)}+\frac{\ell-1}{3}$$
$$+\frac{(p^{2\ell-2}-1)(p-2)}{4(p^2-1)}-\frac{p^{\ell-1}-\ell}{4}+\frac{(p-3)\left(p^{2\ell-1}-2p^{2\ell-2}-3p^{\ell}-3p^{\ell-1}+2p+5\right)}{24(p^2-1)}$$
$$+\frac{p(p^{\ell-2}-1)}{2(p-1)}-\frac{\ell-2}{2}+\frac{(p^{\ell-1}-1)(p-3)}{4(p-1)}+\frac{p^{2\ell-2}-1}{8(p^2-1)}-\frac{\ell-1}{8}$$
$$=\frac{p^{2\ell+2}+p^{2\ell+1}+p^{2\ell}-3p^{\ell+2}-6p^{\ell+1}-3p^{\ell}-p^2(\ell-2)+5p+\ell+2}{24\,(p^2-1)}.$$

The theorem is shown. □

We end with Table 1 displaying the number of equivalence classes for dimension p^{ℓ}, where $3 \leq p \leq 31$, and powers $1 \leq \ell \leq 5$. As an example, the actual computation (using a program supplied by T.W. Cusick and his students) for $n = 7^3$ took 10.5 hours on an Windows 7 Pro `i7` with 16GB of memory, however, for $n = 5^4$, the program did not finish the computation after 6 days. Interestingly, our formulas agree with all these computations for smaller powers (in spite of the fact that we had to impose the bound $p \geq 29$ in our main theorem) and so, we used our formulas to quickly compute the number of classes for higher powers (we put an asterisk next to that count).

Acknowledgement. The author would like to thank T.W. Cusick for some useful suggestions and for his help with a Mathematica code. Also, thanks are due to the referee for providing some useful suggestions.

References.

Table 1: The number of equivalence classes for p^ℓ, $3 \le p \le 31$, $1 \le \ell \le 5$

p \ n	1	2	3	4	5
3	0	4	44	426	3940
5	1	30	819	20908*	524997*
7	2	112	5766	284840*	13973842*
11	4	658	81612*	9897016*	1197780520*
13	7	1274	218757*	37019332*	6256916099*
17	11	3670	1071393*	309820076*	89541196087*
19	14	5698	2073642*	748909856*	270362647330*
23	20	12140*	6458556*	3417415664*	1807832195324*
29	33	30446*	25695699*	21612733932*	18176386152005*
31	38	39676*	38246514*	36758592152*	35325121572190*

[1] A. Biryukov, C. De Cannière, A. Braeken, B. Preneel, A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms, *Advances in Cryptology – Eurocrypt* 2003, LNCS 2656 (E. Biham, ed.), Springer–Verlag, 2003, 33–50.

[2] D. Canright, J.H. Chung, P. Stănică, Circulant Matrices and Affine Equivalence of Monomial Rotation Symmetric Boolean Functions, to appear.

[3] T.W. Cusick, Affine equivalence of cubic homogeneous rotation symmetric functions, *Inform. Sci.* 181:22 (2011), 5067–5083.

[4] T.W. Cusick, A. Brown, Affine equivalence for rotation symmetric Boolean functions with p^k variables, *Finite Fields Applic.* 18:3 (2012), 547–562.

[5] T.W. Cusick and Y. Cheon. Affine equivalence for rotation symmetric Boolean functions with 2^k variables, *Designs, Codes and Cryptography* 63 (2012), 273–294.

[6] T.W. Cusick, Y. Cheon Affine equivalence of quartic homogeneous rotation symmetric Boolean functions, *Inform. Sci.* 259 (2014), 192–211.

[7] T.W. Cusick, P. Stănică, Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions, *Discrete Mathematics* 258 (2002), 289–301.

[8] A. Maximov, M. Hell, S. Maitra, Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables, *International Workshop on Boolean Functions: Cryptography and Applications* (BFCA 2005), University of Rouen, France (2005); available at eprint.iacr.org, no. 2004/144, 2004.

[9] A. Maximov, Classes of Plateaued Rotation Symmetric Boolean functions under Transformation of Walsh Spectra, *Workshop on Coding and Cryptology* 2005 (O. Ytrehus, ed.), LNCS 3969 (2006), 325–334.

[10] J. Pieprzyk, C.X. Qu, Fast Hashing and Rotation-Symmetric Functions, *J. Universal Computer Science* 5 (1999), 20–31.

[11] P. Stănică, S. Maitra, Rotation Symmetric Boolean Functions – Count and Cryptographic Properties, *Discrete Appl. Math.* 156 (2008), 1567–1580.

[12] D. Wiedemann, M.E. Zieve, Equivalence of sparse circulants: the bipartite Ádám problem, http://arxiv.org/abs/0706.1567.